Amendments to the Specification:

[0001] This patent application claims the benefit of U.S. Provisional Application Nos. 60/284,163 filed April 16, 2001, entitled "Watermark Systems and Methods," and 60/284,776 filed April 18, 2001, entitled "Using Embedded Identifiers with Images." This application is also a continuation-in-part of assignee's U.S. Patent Application No. 09/800,093 (published as US 2002-0124171 A1), entitled "Geo-Referencing of Aerial Imagery Using Embedded Image Identifiers and Cross-Referenced Data Sets," filed March 5, 2001.

A1

[0002] This patent application is also related to assignee's U.S. Patent Application No. 09/833,013 (published as US 2002-0147910 A1), entitled "Digitally Watermarked Maps and Signs and Related Navigational Tools," filed April 10, 2001.

[0036] In some instances, user terminal 18 will create additional derivatives. Take for instance, an example when user terminal 18 enlarges the derivative 001 image, thus creating a new derivative 001a. This new derivative is preferably uniquely identified ~~identifiers~~ with a digital watermark. A process of digitally watermarking a derivative typically involves removing the original watermark from the derivative and replacing the watermark with a new unique identifier. (In an alternative embodiment, the original watermark is altered, e.g., by changing one or more message bits, to create the new unique identifier. In another embodiment, a second watermark is added to the derivative image to complement the first (or more) watermark. In this case, the first watermark identifies the original image, and the second watermark identifies the derivative.). Preferably, upon creating derivative 001a, the digital watermarking software removes the derivative 001 watermark (or at least a portion of the watermark, e.g., identifier ID-5) from the derivative 001 image. Assignees' U.S. application 09/503,881 discusses some techniques for such. Artisans know others still. Derivative 001a is then embedded with a unique digital watermark identifier (e.g., ID-10).

A2

[0043] There are often situations where it is desirable to carry some form of security access indicator in an image, e.g., via a digital watermark. The security access indicator defines a level of security required to view, edit or comment with respect to an image. Access to the image is then controlled by appropriately enabled software, which extracts the indicator (or receives the indicator from a watermark decoder) and determines usage. In one embodiment, the indicator indicates or defines a required level. If a user's security level is equal to or greater (e.g., as determined from a password, user terminal identifier, login, linked security clearance level, etc.) to that carried in a security access indicator, then a user is allowed access to the image or data. In another embodiment, a security code may indicate that a particular user can view the image, but cannot edit or store comments regarding such.

A5